CHAPTER 7

SAFEGUARDING

7-1 BASIC POLICY

1. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited AISs, and under conditions which prevent unauthorized persons from gaining access. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified information is processed or stored. These areas may be designated, in writing, by the commanding officer as restricted areas per reference (a). Decisions regarding designations of restricted areas, their levels, and criteria for access are at the discretion of the commanding officer. All personnel shall comply with the **need-to-know** policy for access to classified information.

2. Classified information is the property of the U.S. Government and not personal property. Military or civilian personnel who resign, retire, separate from the DON, or are released from active duty, shall return all classified information in their possession to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers.

7-2 APPLICABILITY OF CONTROL MEASURES

Classified information shall be afforded a level of control commensurate with its assigned security classification level. This policy encompasses all classified information regardless of media.

7-3 TOP SECRET CONTROL MEASURES

1. All Top Secret information (including copies) originated or received by a command shall be continuously accounted for, individually serialized, and entered into a command Top Secret log. The log shall completely identify the information, and at a minimum include the date originated or received, individual serial numbers, copy number, title, originator, number of pages, disposition (i.e., transferred, destroyed, transmitted, downgraded, declassified, etc.) and date of each disposition action taken.

2. In addition to the marking requirements of chapter 6, Top Secret information originated by the command shall be marked with an individual copy number in the following manner "Copy No. ____ of ____ copies." Exceptions to this rule are allowed for publications containing a distribution list by copy number and for mass-produced reproductions when copy numbering would be cost prohibitive. In the latter case, adequate and readily available documentation shall be maintained indicating the total copies produced and the recipients of the copies.

3. TSCOs shall obtain a record of receipt (typically a classified material receipt) from each recipient for Top Secret information distributed internally and externally.

4. Top Secret information shall be physically sighted or accounted for at least annually, and more frequently as circumstances warrant (e.g., at the change of command, change of TSCO, or upon report of loss or compromise). As an exception, repositories, libraries or activities which store large volumes of classified material may limit their annual inventory to all documents and material to which access has been given in the past 12 months, and 10 percent of the remaining inventory. See chapter 2, paragraph 2-3 for TSCO duties.

7-4 SECRET CONTROL MEASURES

Commanding officers shall establish administrative procedures for the control of Secret information appropriate to their local environment, based on an assessment of the threat, the location, and mission of their command. These procedures shall be used to protect Secret information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this regulation.

7-5 CONFIDENTIAL CONTROL MEASURES

Commanding officers shall establish administrative procedures for the control of Confidential information appropriate to their local environment, based on an assessment of the threat, location, and mission of their command. These procedures shall be used to protect Confidential information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this regulation.

7-6 WORKING PAPERS

1. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents. Working papers that contain classified information shall be:

a. Dated when created;

b. Conspicuously marked "**Working Paper**" on the first page in letters larger than the text;

c. Marked centered top and bottom on each page with the highest overall classification level of any information they contain;

d. Protected per the assigned classification level; and

e. Destroyed, by authorized means, when no longer needed.

2. Commanding officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

7-7 SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION

1. Control and safeguard special types of classified information as follows:

a. **NWPs**. Reference (b) requires an administrative system for controlling the NWP Library within the command. Classified NWPs shall be safeguarded per this chapter, according to their security classification level. Administrative controls for NWPs do not replace the security controls required for classified information.

b. **NATO**. Control and safeguard NATO classified information (including NATO Restricted) per reference (c).

c. **FGI.** Control and safeguard FGI, other than NATO, in the same manner as prescribed by this regulation for U.S. classified information, except as follows:

(1) FGI controls and safeguards may be modified as required or permitted by a treaty or international agreement, or by the responsible national security authority of the originating government for other obligations that do not have the legal status of a treaty or international agreement (e.g., a contract).

(2) **TOP SECRET FGI.** Maintain records for the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmission of Top Secret FGI. The originating government shall approve reproduction, and destruction shall be witnessed by two appropriately cleared personnel. Retain records for 5 years.

(3) **SECRET FGI.** Maintain records for the receipt, transmission and destruction of Secret FGI. Secret FGI may be reproduced to meet mission requirements and reproduction shall be recorded. Retain records for 3 years.

(4) **CONFIDENTIAL FGI.** Maintain records for the receipt and transmission of Confidential FGI. Other records need not be maintained unless required by the originating government. Retain records for 2 years.

(5) **FOREIGN GOVERNMENT RESTRICTED and UNCLASSIFIED INFORMATION PROVIDED IN CONFIDENCE.** The degree of protection provided to the FGI shall be at least equivalent to that required by the foreign government. If the foreign government protection requirement is lower than the protection required for U.S. Confidential information observe the following rules:

(a) Provide the information only to those who have a need-to-know;

(b) Notify individuals given access of applicable handling instructions in writing or by an oral briefing; and

(c) Store information in a locked desk or cabinet, or in a locked room to which access is controlled to prevent unauthorized access.

d. **RD (INCLUDING CNWDI) and FRD.** Control and safeguard RD and FRD per reference (d).

e. **SCI.** Control and safeguard SCI per reference (e).

f. **COMSEC.** Control and safeguard COMSEC information per references (f) and (g).

g. **SIOP and SIOP-ESI.** Control and safeguard SIOP and SIOP-ESI per reference (h).

h. **SAPs.** Control and safeguard SAP information per reference (i).

i. **NNPI.** Control and safeguard NNPI per reference (j).

j. **FOUO.** Control and safeguard FOUO information per reference (k).

k. **SBU INFORMATION.** Control and safeguard SBU information in the same manner as FOUO, per reference (k).

l. **DEA SENSITIVE INFORMATION.** Control and safeguard DEA Sensitive information in the same manner as FOUO, per reference (k).

m. **DoD UCNI.** Control and safeguard DoD UCNI per reference (l).

n. **SENSITIVE INFORMATION (COMPUTER SECURITY ACT OF 1987).** Control and safeguard Sensitive Information contained in U.S. Government AISs per reference (m).

7-8 ALTERNATIVE OR COMPENSATORY CONTROL MEASURES

1. The CNO (N09N) approves the use of alternative or compensatory security control measures and ensures that the protection afforded classified information is sufficient to reasonably deter and detect loss or compromise. Upon request, OCAs shall furnish to other DoD components or executive branch agencies, with whom classified information or secure facilities are shared, approvals for alternative or compensatory control measures. The CNO (N09N2) will provide a copy of this documentation to the DUSD(PS) or ASD(C^3I) as appropriate, for reporting to the Director, ISOO.

2. Requests for approval of such controls shall include criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and countermeasures benefits versus cost.

3. The CNO (N09N2) shall maintain a centralized record that, as a minimum, reflects the control(s) used and the rationale for their use. Controls include:

a. Maintenance of lists or rosters of personnel to whom the classified information has been or may be provided;

b. Using a nickname to identify classified information which requires alternative or compensatory protection. A code word shall not be used for this purpose. Other special terminology or special markings shall not be used except that prescribed for the handling of messages.

c. Requiring that classified information be placed in sealed envelopes marked only with the nickname and stored in a manner to avoid combining with other classified information.

d. Requiring unique DoD component oversight or inspection procedures.

4. Approved controls may be applied to cleared DoD contractors only when identified in the DD 254.

5. Alternative or compensatory security control measures shall not be applied to RD (including CNWDI), FRD, SIOP or SIOP-ESI information.

6. Requests to use alternative or compensatory security control measures for the safeguarding of NATO or FGI shall be submitted to the DUSD(PS) via the administrative chain of command and the CNO (N09N2).

7. Alternative or compensatory security control measures shall not preclude, nor unnecessarily impede, Congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

7-9 CARE DURING WORKING HOURS

1. Keep classified information under constant surveillance by an authorized person or covered with SFs 703, 704, or 705 when removed from secure storage.

2. In a mixed working environment (i.e., classified and unclassified), AIS media used for processing or storing classified information shall be marked with an SF 706, 707,

708, 709, 710, 711, or 712 (SCI), as applicable. In a totally unclassified working environment, SF labels are not required.

3. Protect preliminary drafts, plates, stencils, stenographic notes, worksheets, computer printer and typewriter ribbons, computer storage media, and other classified items according to their security classification level. Immediately destroy these items after they have served their purpose.

4. Classified discussions shall not be conducted with or in the presence of unauthorized persons. Take special care when visitors are present. Practice the need-to-know principle.

7-10 END-OF-DAY SECURITY CHECKS

Commanding officers shall establish procedures for end of the day security checks, utilizing the SF 701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, an SF 702, Security Container Check Sheet, shall be utilized to record that classified vaults, secure rooms (strong rooms), and containers have been properly secured at the end of the day. The SF 701 and 702 shall be annotated to reflect after hours, weekend, and holiday activities in secure areas.

7-11 SAFEGUARDING DURING VISITS

Commanding officers shall establish procedures to ensure that only visitors with an appropriate clearance level and need-to-know are granted access to classified information. At a minimum, these procedures shall include verification of the identity, clearance level, access (if appropriate), and need-to-know for all visitors. Refer to reference (n) for visit procedures.

7-12 SAFEGUARDING DURING CLASSIFIED MEETINGS

1. Commanding officers shall ensure that classified discussions at conferences, seminars, exhibits, symposia, conventions, training courses, or other gatherings (hereafter referred to as "meetings") are held only when disclosure of the information serves a specific U.S. Government purpose. Classified meetings shall be held only at a U.S. Government agency or a cleared DoD contractor facility with an appropriate facility security clearance (FCL) where adequate physical security and procedural controls have been approved.

2. Commands hosting in-house meetings attended by members of the command and authorized visitors shall assume security responsibility for the meeting. Take precautions for conference rooms and areas specifically designated for classified discussions. Request technical surveillance counter-measures support for conferences involving Top Secret information, and for other designated classified discussion areas per reference (o).

3. Commands hosting meetings outside the command, including those supported by non-U.S. Government associations, shall:

a. Confirm that other means for communicating or disseminating the classified information in lieu of a meeting are inadequate;

b. Ensure that attendance is limited to U.S. Government personnel or cleared DoD contractor employees. Any participation by foreign nationals or foreign representatives shall be approved, in writing, by the DON command foreign disclosure office or Navy IPO prior to attendance to ensure that the information to be presented has been cleared for foreign disclosure. All attendees shall possess an appropriate level of clearance and need-to-know;

c. Prepare and implement a security plan that minimizes the risk to the classified information involved;

d. Segregate classified sessions from unclassified sessions;

e. Ensure that announcements are unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions when non-U.S. Government associations are providing administrative support;

f. Permit note taking or electronic recording during classified sessions only when the sponsor determines, in writing, that such action is necessary to fulfill the U.S. Government purpose for the meeting; and

g. Safeguard, transmit, or transport classified information created, used, or distributed during the meeting per this chapter and chapter 9.

4. Command personnel invited to give classified presentations or to accept security sponsorship for classified meetings organized by non-U.S. Government associations must receive approval from

the CNO (N09N2) prior to any commitment or announcement being made. Requests to conduct such meetings shall be forwarded to the CNO (N09N2) via the administrative chain of command and shall include:

a. A summary of subjects, level, and sources of classified information;

b. The name of the non-U.S. Government association or organization involved in the meeting;

c. The location and dates of the meeting;

d. Identification of the sponsoring command, including the name, address, and phone number of the primary action officer;

e. The specific reason for having the meeting;

f. A security plan specifying procedures for processing security clearances, badging procedures, access control procedures, and procedures for storing the classified information;

g. A draft agenda, announcement, and clearance verification form;

h. The identity of any foreign representatives expected to attend, with proof of their official clearance level assurance and a statement of their need-to-know.

5. Pending a decision by the CNO (N09N2), general notices or announcements of meetings may be published or sent to members of participating associations, societies, or groups if the notice or announcement does not constitute an invitation to attend. If approval is granted, the CNO (N09N2) shall appoint a U.S. Government official to serve as security manager for the meeting. The security manager shall provide and maintain physical security for the actual site of the classified meeting. Other U.S. Government organizations or cleared contractor facilities with an appropriate level FCL may assist with implementation of security requirements under the direction of the appointed security manager. Upon assuming security sponsorship, the sponsor shall review all announcements and invitations to determine that they are accurate, do not contain classified information, and clearly identify the security sponsor.

7-13 REPRODUCTION

1. U.S. classified and DEA Sensitive unclassified information shall be reproduced only to the extent required by operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives. See paragraph 7-7.3 for reproduction of FGI.

2. Commanding officers shall:

a. Designate specific equipment for classified reproduction;

b. Limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk;

c. Comply with reproduction limitations placed on classified information by originators and special controls applicable to special types of classified information;

d. Facilitate oversight and control of reproduction; and

e. Ensure the expeditious processing of classified information in connection with review for declassification.

REFERENCES

(a) OPNAVINST 5530.14C, *DON Physical Security and Loss Prevention*, 10 Dec 98 (NOTAL)

(b) NWP 1-01, *Naval Warfare Publications System*, Hardcopy Nov 1994/CD-ROM Dec 97 (NOTAL)

(c) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(d) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(e) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(f) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(g) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)

(h) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(i) OPNAVINST S5460.4C, *Control of Special Access Programs Within the DON (U)*, 14 Aug 81 (NOTAL)

(j) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(k) SECNAVINST 5720.42E, *DON Freedom of Information Act, (FOIA) Program*, 5 Jun 91

(l) OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI)*, 11 Feb 93

(m) Title 5 of Public Law 93-579, *The Privacy Act*, U.S.C., Section 552a

(n) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(o) SECNAVINST 5500.31A, *Technical Surveillance Countermeasures (TSCM) Program*, 4 Jun 85 (NOTAL)